تكييف الهجمات السيبرانية في ضوء القانون الدولي

Adjusting Cyber Attacks in the Light of International Law

أ.د. أحمد عبيس نعمة

نبذة عن الباحث :
استاذ القانون الدولي في كلية القانون جامعة الكوفة.

زهراء عماد محمد كلنتر

نبذة عن الباحث :
طالبة ماجستير .

تاريخ استلام البحث :
٢٠١٨/٠٣/٠٢
تاريخ قبول النشر :
٢٠١٨/٠٣/١٩

الكلمات الافتتاحية :
الهجمات السبرانية ، القانون الدولي.
Cyber Attacks, International Law

Abstract

The Tremendous electronic development that we are living today led to emergence new challenges in the international community, and one of these challenges is the (cyber attacks), that characterized by easily implemented, thus it became possible for states influence on each other by attack basic infrastructure with one button push and although creating destructive effects whether the size of mass of human or physical.

The Exact feature of cyber attacks is still undefined and so devoted this study for search in concept of this attacks and harmonization between them and international law rules, whether codified and customary

الملخص

إن التطور الإلكتروني الهائل الذي نعيشه اليوم أدى الى نشوء تحديات جديدة في المجتمع الدولي و من هذه التحديات(الهجمات السيبرانية) التي تتميز بسهولة تنفيذها. فأصبح بإمكان الدول التأثير على بعضها البعض عن طريق الهجوم على البنية التحتية الأساسية بكبسة زر واحدة و رغم ذلك إحداث آثار مدمرة سواء في الحجم الدمار البشري أو المادي. إن المعالم الدقيقة للهجمات السيبرانية لازالت غير محددة لذلك خصصنا هذه الدراسة للبحث في مفهوم الهجمات السيبرانية و الموائمة بينها و بين قواعد القانون الدولي المكتوبة منها و العرفية

المقدمة

إن ظهور الشبكة العنكبوتية التي تتميز بسرعة توفير المعلومات أدى الى إنتقال العديد من وسائل السيطرة والتحكم الخاصة بمعظم العمليات الحيوية الموجودة على الأرض الى الفضاء في صورة أقمار إصطناعية ومحطات فضائية، و إنتقل أيضا قطاع واسع من النزاعات المسلحة الى العالم الإفتراضي الذي صنعه الإنسان منذ إختراعه الكمبيوتر والذاكرات الإلكترونية وشبكات المعلومات، فأنشأ داخله جغرافية إفتراضية جديدة. إن هذا الإعتماد المتزايد على الشبكة في معظم أمور الحياة من إقتصاد وثقافة وإجتماع، الى جانب تسهيل وتسريع إنجاز المهام اليومية، قد زاد من المخاطر أيضا، فهذا التطور أتاح سبل جديدة في التعامل الدولي لم تكن ملحوظة أو متوقعة عند وضع النظم القانونية السائدة، فبعد إن كان التعامل الدولي خلال النزاعات المسلحة يتم على الأرض أو الجو أو البحر، أصبح بفضل هذه التقنيات يتم بطريقة إلكترونية ضمن نظام معلوماتي يختلف كليا عن النزاعات المسلحة التقليدية، و أصبحت الشبكة العنكبوتية ساحة نزاعات و صراعات يدخل في سياقها التجسس و الإختراق و التحكم في قواعد بيانات قد تمس الأمن القومي و الحيوي للدول.

إن الهجمات السيبرانية هي إحدى السبل و الأساليب المؤثرة التي نتجت عن هذا التطور الإلكتروني الهائل، و تتميز بسهولة تنفيذها، فأصبح بإمكان الدول التأثير على بعضها عن طريق شل الأنظمة المصرفية أو الأمنية أو العسكرية بكبسة زر واحدة عن بعد دون تكبد العناء و من دون وقوع خسائر مادية أو بشرية في صفوفها ، الا إن ما تحققه من دمار في الدولة المعتدى عليها قد يفوق آثار النزاع المسلح التقليدي سواء في الأرواح البشرية أم في البنى التحتية.

المطلب الأول: مفهوم الهجمات السيبرانية

إن التحدي الأول في تقويم أحكام القانون الوطني والدولي في تنظيم الهجمات السيبرانية، يتجسد في تحديد مفهوم و طبيعة المسألة التي نواجهها، فالنشاطات التي تحدث في الفضاء السيبراني (Cyber Space) ، الذي يعد المجال الخامس بعد البر والبحر والجو والفضاء ، قد لا تتطابق مع المبادئ التقليدية التي تحكم المجتمع الدولي في إطار القانون الدولي العام. وعدم الوضوح هذا يمكن أن يجعل من عملية وضع التكييف القانوني أمراً في غاية الصعوبة.

الفرع الأول: التعريف بالهجمات السيبرانية

لأكثر من عقد من الزمن تكهن المحللون بشأن عواقب محتملة و أضرار مادية و إقتصادية واسعة النطاق نتيجة التطور الإلكتروني ، كإنهيار السدود أو تعطيل سوق الأسهم او إيقاف مفاعل نووي أو تفجيره عن بعد، أو إنقطاع التيار الكهربائي لنظام الملاحة الجوية فضلا عن التلاعب بمسار مرور الطائرات المدنية، وغيرها من الحوادث التي تجري بفعل تقنيات غير مألوفة على الصعيد الدولي، و على الرغم مما تقدم لا يوجد تعريف ثابت ليشمل تلك الحوادث، وإن عدم وجود تعريف مشترك جعل من الصعب

على المحللين في مختلف البلدان وضع توصيات منسقة أو إتفاق الدول على مبادئ موحدة لمنع او التقليل من حدوث هذه الكوارث[١].

أولا : تعريف الهجمات السيبرانية

إن تعريفات الهجمات السيبرانية القائمة والمفاهيم ذات الصلة واسعة جداً، إلا إن هناك إتجاهين رئيسيين مختلفين[٢] في تعريف هذا النمط من الهجمات و هما :الإتجاه الضيق الذي يركز على موضوع الهجوم، وهذا ما تبنته الولايات المتحدة الأمريكية و حلفاؤها. ومن أمثلة التعريفات في هذا الإتجاه، ما تبنته القيادة الإستراتيجية الأمريكية عام ٢٠٠٧ بشأن إستخدام الوسائل الإلكترونية للأغراض العسكرية. فقد عرفته بأنه: "تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الإستخدام الفعّال لها، فضلاً عن التسلل الى أنظمة المعلومات وشبكات الإتصال بهدف جمع البيانات التي تحتويها و حيازتها و تحليلها"[٣].

أما التعريف الذي طرحه البروفيسور فيورتس (Fuertes) الأستاذ في قسم الكيمياء في جامعة تكساس للتكنولوجيا فهو: "هجوم عبر الإنترنيت يقوم على التسلل الى مواقع الكترونية غير مرخص بالدخول اليها، بهدف تعطيل البيانات المتوفرة أو إتلافها أو الإستحواذ عليها وهي عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد أخرى"[٤].

على النقيض من الإتجاه الضيق الذي تبنته الولايات المتحدة رسمياً، فقد تبنت منظمة شنغهاي للتعاون نهجاً أكثر توسعاً بشأن الهجمات السيبرانية. حيث أعربت هذه المنظمة عن قلقها بشأن التهديدات التي تشكلها إمكانية إستخدام وسائل المعلومات والإتصالات الحديثة و تقنياتها لأغراض تتنافى مع ضمان الأمن والإستقرار الدوليين على الصعيدين العسكري والمدني[٥]. فينظر أعضاء هذه المنظمة – أي مؤيدي الإتجاه الواسع – الى نشر المعلومات الضارة للأنظمة الإجتماعية والسياسية والإجتماعية والإقتصادية، فضلاً عن المجالات الروحية والأخلاقية والثقافية للدول الأخرى بوصفها أيضاً من التهديدات الرئيسية للأمن السيبراني[٦].

إن التعارض في محتوى هذين الإتجاهين – في مفهوم الهجمات السيبرانية- يظهر الحاجة الماسة إلى وضع تعريف واضح ومتفق عليه دوليا بشان تلك الهجمات.

إن الهجوم السيبراني تصرف يدور في عالم رقمي قائم على إستخدام بيانات رقمية و وسائل إتصال تعمل الكترونياً، ومن ثم تطور ليتضمن مفهوماً أوسع يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جراء إختراق مواقع الكترونية حساسة، عادة ما تقوم بوظائف تصنف بأنها ذات أولوية، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات و وسائل النقل الأخرى[٧].

و على وفق ما تقدم نرى إن التعريف الذي أورده شميت (Schmitt) المتخصص في القانون الدولي الإنساني والعضو البارز في مركز الدفاع السيبراني التعاوني التابع لحلف الشمال الأطلسي(NATO) في دليل تالين هو الأقرب لمفهوم الهجمات السيبرانية، إذ عرفها بالقول : "الهجوم السيبراني هو أي تصرف الكتروني دفاعياً كان أم هجومياً يتوقع

منه وعلى نحو معقول في التسبب بجرح أو قتل شخص أو إلحاق أضرار مادية أو دمار بالهدف المهاجم"[٨].

ثانيا: تمييز الهجمات السيبرانية عن مصطلحات مشابهة

فيما يأتي من البحث سنحاول إبداء أوجه التمييز بين مصطلح الهجمات السيبرانية (Cyber Attacks) ومصطلحات أخرى إستخدمت بشأن وسائل الهجوم الإلكترونية منها: الجريمة السيبرانية (Cyber Crime) و التي تعرف بأنها : "هي الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لإرتكابها أو يمثل إغراءاً بذلك، أو جريمة يكون الحاسب الآلي نفسه ضحيتها"[٩]. إن الجريمة السيبرانية لا تشمل فقط الجرائم التي ترتكب عن طريق الكمبيوتر، بل تشمل أيضاً أية جريمة تتضمن إستخدام أو إستهداف الكمبيوتر[١٠]. و تاكيدا على ذلك ما جاء في إرشادات الإسكوا (ESCWA)[١١] للتشريعات السيبرانية في بيان مفهوم الجريمة السيبرانية إذ ذهب إلى: "إن الجريمة السيبرانية تنقسم على نوعين أساسيين : النوع الأول هو الذي يكون فيه الحاسوب أداة تنفذ بواسطتها الجريمة ، و النوع الثاني هو الذي يكون فيه جهاز الحاسوب و شبكات الحواسيب و برامجها موضوعا للجريمة، أي: إن الفعل الجرمي إرتكب على هذا الجهاز"[١٢].

و قد ترتكب الجريمة السيبرانية لعدة أغراض كتحقيق مكاسب مادية معينة أو لإثبات الفاعل لمهارته الفنية و قدرته على إختراق أجهزة الحاسب أو بهدف التسلية و الترفيه أو لمجرد الرغبة في الإضرار بالغير [١٣]. ومن أمثلة الجرائم السيبرانية، الممارسات الإحتيالية على الإنترنيت ، مشاركة الصور الإباحية للأطفال وتخزينها على الكمبيوتر و القذف و السب عبر الوسائل الإلكترونية و غيرها من النشاطات المخالفة بموجب القوانين الوطنية.

إن الجرائم السيبرانية و إن كانت تشترك مع الهجمات السيبرانية في البيئة التي تحدث فيه أي الفضاء السيبراني، إلا إنها تختلف عنها من حيث الأشخاص و الأهداف، فغالباً ما يكون مرتكبي الجرائم السيبرانية هم الأفراد و توجة ضد مؤسسات مالية أو شركات وحتى أفراد داخل أو خارج إقليم الدولة بخلاف الهجمات التي تتم من قبل دول أو مجموعات حكومية أو غير حكومية ضد دولة أخرى[١٤]. إن الإختلاف الآخر يكمن في إن الجرائم السيبرانية غالباً ما يكون الهدف منها تحقيق مكاسب شخصية كسرقة الملكية الفكرية عن طريق شبكات الحاسب الآلي أو التسلل الى أنظمة المصارف و التلاعب بأرقام الحسابات و تحويل الأموال ، بخلاف الهجمات السيبرانية التي يستهدف مرتكبوها الأمن القومي و السياسي للدولة أو يقوم هؤلاء بتخريب الشبكات التي تتحكم بالبنى التحتية الأساسية في الدولة و تدميرها بقصد إرباكها، و زعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية[١٥].

إن المصطلح المشابه و المقارب الأخر هو الحرب السيبرانية (Cyber Warfare) الذي يعد مفهوما جديدا على صعيد النزاعات المسلحة في القرن الحادي و العشرين ، فهذه الحرب

تشتمل على أساليب و وسائل قتالية تتألف من عمليات إلكترونية ترقى الى مستوى النزاع المسلح أو تستخدم في سياقه. إن الحرب السيبرانية هي الإخلال أو التدمير الكلي لأنظمة المعلومات و الإتصالات التابعة للعدو التي يعتمد عليها كما تهدف الى الإخلال بتوازن المعلومات والمعرفة لصالح القوات الصديقة، لاسيما في غياب التوازن العسكري. و عرفتها مؤسسة راند(RAND)[١٦] بأنها : " حرب الدول و المنظمات الدولية ضد دول أخرى من أجل تدمير شبكات الكمبيوتر و المعلومات . و هذه الحرب تتم عن طريق الفايروسات ، أحصنة طروادة و البرمجيات الخبيثة الأخرى"[١٧].

إن الحرب السيبرانية لها من الخصائص ما يميزها عن النزاعات المسلحة التقليدية سواء من حيث ماهيتها أم مضمونها، فبخلاف النزاعات المسلحة التقليدية لا يمكن تحديد وقت بدء الحرب السيبرانية أو إنتهائها، بل إن فاعلية الحرب السيبرانية تكمن في عدم إمكانية تحديد وقت بدءها[١٨]. إن صعوبة التوصل و معرفة مصدر الحرب السيبرانية تشكل عامل إختلاف آخر و ذلك لعدة أسباب، منها تعدد الجهات الفاعلة في الفضاء السيبراني كالدول و المنظمات و الجماعات الحكومية و غير الحكومية و الإرهابيين و القراصنة و حتى الأفراد[١٩].

مما سبق يتبين إن الحرب السيبرانية و إن كانت تتفق كثيرا مع الهجمات السيبرانية، إلا إن ذلك لا يعني عدم وجود ما يميزهما عن بعض، فالحرب السيبرانية هي نوع أو جزء من الهجمات السيبرانية التي تحدث في أثناء نزاع مسلح دائر أو التي تنتج آثارا مادية (أو مايسمى بالآثار الحركية) تشبه و تعادل آثار الهجمات المسلحة التقليدية ؛ بينما الهجمات السيبرانية هي كل نشاط إلكتروني ضار بالدول الأخرى سواء كان في وقت السلم أم في أثناء نزاع مسلح دائر و سواء نتجت عنه أثار مادية جسيمة في الأرواح أم الممتلكات أو لم يؤدي إلا الى تشويش أنظمة الكمبيوتر فيها مادام كان ذلك لأغراض أمنية و عسكرية و أحدث إرباك في عمل الحكومة التابعة لتلك الدولة[٢٠].

الفرع الثاني: طبيعة الهجمات السيبرانية

لدى التعرض الى تعريف الهجمات السيبرانية ، فإن تساؤلات عدة تطرح بخصوص طبيعة هذه الهجمات، هل تعد وسيلة للقتال ام هي إسلوب تلجأ اليه الأطراف المتنازعة، بعبارة أخرى هل يمكن عدها سلاحاً أم هي طريقة قتالية. للإجابة عن هذه التساؤلات فلابد اولاً بيان مفهوم وسائل و طرق القتال، كما لابد من الرجوع الى أحكام الصكوك الدولية ذات الصلة بتنظيم النزاعات المسلحة التقليدية. فحسب رأي موريس اوبير(Murice Abuert) : "إن وسائل القتال هي الأسلحة ذاتها بينما كيفية إستخدامها تشكل طرائقها"[٢١]. كما إن هناك إتفاقيات عديدة بشأن تنظيم إستخدام الأسلحة لاسيما الحديثة والمتطورة منها، التي يمكن أن تنطبق الى حد ما على الهجمات السيبرانية[٢٢]. قد بينت مفهوم الأسلحة(وسائل القتال).

إن الأسلحة هي الأدوات التي تستخدم من قبل القوات العسكرية في أثناء القتال[٢٣] . وقد جاء تعريف الأسلحة التقليدية في قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبناء الثقة الصادر عن الأمم المتحدة بأنها: "أسلحة ليست أسلحة تدمير

شامل، جرى فهمها على أنها تتضمن أجهزة مصممة للقتل أو الجرح أو إلحاق الضرر، عادة لا حصراً، بواسطة تأثيرات المواد شديدة الإنفجار أو الطاقة الحركية أو العوامل المحرقة ونظم إيصالها"[٢٤].

و من جهة أخرى هناك أسلحة دمار شامل (Weapons of Mass Destruction) والتي تعرف بأنها "أي نوع سلاح كيميائي، بيولوجي و نووي، و الذي يكون قادرا على إحداث تدمير واسع في الأرواح و الأموال عن طريق إستخدام المواد الكيميائية و البيولوجية و الراديوم"[٢٥].

إن الهجمات السيبرانية قد تستخدم لتعطيل أو تدمير الأجهزة الإلكترونية المسؤولة عن تنظيم شبكة الكهرباء أو المياه و السدود أو المفاعل النووية أو غيرها من المنشآت الحيوية مما قد يعرض صالح الكثير من المدنيين أو حياتهم للخطر. ومن ناحية أخرى كثيراً ما يتم اللجوء الى الهجمات السيبرانية لتسهيل تنفيذ هجمات مسلحة تقليدية أي يتم إستخدام هذه الهجمات لتعطيل شبكات الإتصال التابعة للخصم لتسهيل وحماية حركة السلاح الجوي لتنفيذ غاراته وإلحاق الضرر بالعدو، أو يتم إستخدامها لتحديد المواقع الحساسة لدى العدو ليتم قصفها وتدميرها.

أولا: الهجوم السيبراني كوسيلة قتالية

إذا تم إستخدام الهجوم السيبراني بذاته للتسلل الى أنظمة الكترونية معدة لحماية أو تنظيم سير عمل منشآت حيوية للسيطرة عليها وتدميرها، فهنا يعد الهجوم السيبراني وسيلة قتالية أي سلاحاً يهاجم به العدو[٢٦].

و خير مثال على ذلك فيروس (Stuxnet) الذي إستخدم في الهجوم على محطات "نطنز" و"بوشهر" النووية الإيرانية و الحق أضراراً جزئية في عملية تخصيب اليورانيوم[٢٧]. و هو عبارة عن برنامج الكتروني معقد للغاية، يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آلياً ويعد هذا الفيروس هو الأول من نوعه، إذ لا يعمل عشوائياً كما هي العادة بل بشكل محدد جداً حيث يخترق الأجهزة والحواسيب بحثاً عن علامة فارقة مبرمج عليها ثم يقوم بتفعيل نفسه عند إيجادها، ويبدأ بالعمل على تخريب المنشأة المستهدفة و تدميرها من خلال العبث بأنظمة التحكم التابعة لتلك المنشأة[٢٨].

إن من أهم الإشكاليات التي تواجه المجتمع الدولي في طريقة التعامل مع الأنشطة الإلكترونية هي ما يتعلق بالجدل حول إمكانية عدّ الأنشطة السيبرانية كسلاح غير تقليدي وإمكانية خضوعها لقيود الإتفاقيات المعنية بالحد من التسلح إذ ذهب بعض الخبراء بعدم صحة وصف الهجمات السيبرانية بأنها "سلاحاً" لأنها تفتقد الى الطاقة الحركية (Kinetic) وبالتالي عدم خضوعها للتنظيمات الدولية المتعلقة بإستخدام الأسلحة.[٢٩]

وهذا مخالف للواقع إذ لا يشترط في الأسلحة إحتواؤها على الطاقة الحركية وخير مثال على ذلك الأسلحة الكيميائية أو البيولوجية. ومما يؤيد هذا ما ذكرته وزارة الدفاع الأمريكية (البنتاغون) عام ١٩٩٩ في تقييم القضايا القانونية الدولية في العمليات

الإعلامية: "إذا ركزنا على المعنى المستخدم قد نتوصل الى إن النشاطات الإلكترونية غير المحسوسة بالحواس البشرية لا تشبه القنابل أو الرصاصات أو الوحدات العسكرية لذلك من المحتمل أن يهتم المجتمع الدولي بنتائج هجمات شبكة الكمبيوتر أكثر من آليتها"[٣٠].

وقد ذهب البعض الآخر من الخبراء الى أبعد من ذلك حيث عمدوا الى إطلاق مصطلح التعطيل الشامل (Mass Disruption)[٣١] على الهجمات السيبرانية لتقابل مصطلح الدمار الشامل (Mass Destruction) الذي يطلق على الأسلحة النووية والكيميائية والبيولوجية، نظراً لآثار الهجوم السيبراني وجسامته في الإضرار والتخريب، و لاسيما آثاره على الحركة الجوية عند تعطيل شبكة الكهرباء، وكذلك خدمات الطوارئ وغيرها من الآثار الجسيمة.

مما تقدم يتبين إن الهجمات السيبرانية تتمتع بما يتصف به أي سلاح آخر، أي: لها عنصر معنوي يتمثل في النية بإيقاع إصابات في الهدف العسكري للعدو وعنصر آخر مادي يتمثل في توجيه السلاح ضد أهداف عسكرية أو مدنية منتخبة[٣٢].

ثانيا: الهجوم السيبراني كطريقة قتالية

إن الهجوم السيبراني إذا أسهم في توجيه العمليات العسكرية وسهّل عمل القوة العسكرية التقليدية، فيعد طريقة قتالية[٣٣]. كالطائرات بدون طيار (Drawn) التي توجه لتحديد أهداف عسكرية منتخبة ومن ثم تدميرها للإخلال في صفوف القوة العسكرية المعادية، أو إستخدام الهجوم السيبراني لإيقاف عمليات الإتصال في المطارات العسكرية والمدنية.

ففي هذه الحالات، لم يستخدم الهجوم السيبراني لتحقيق الهدف بنفسه بل لتمهيد الطريق أمام القوات العسكرية لتحقيق ميزة أو أفضلية عسكرية على العدو، فلذلك يمكن عدّها طريقة قتالية و إدراجها ضمن التخطيطات والتكتيكات العسكرية. ومن الأمثلة على ذلك ما قامت به اسرائيل عام ٢٠٠٧ ضد سوريا، حيث لجأ سلاح الجو الاسرائيلي الى إستخدام تكنولوجيا متقدمة جداً تمكن بموجبها من إختراق منظومات الإتصال وأجهزة الرادار التابعة للقوات السورية، لمنع إكتشاف طائراتها، فظهرت السماء صافية في الرادارات السورية في الوقت الذي كانت تحلق طائرات اسرائيلية في المجال الجوي السوري وتقوم بتفجير وتدمير أهداف، كانت بناء على الإستطلاعات الاسرائيلية مشروعا لإنشاء مركز ذات نشاطات نووية غير مدنية حسب ما إدعت إسرائيل بذلك.[٣٤]

من كل ما تقدم يتبين إن الهجمات السيبرانية تشكل وسيلة وطريقة قتالية في الوقت نفسه وذلك على وفق الأهداف المستخدمة لتحقيقها، و تخضع هذه الهجمات الى المادة ٣٦من البروتوكول الإضافي الأول لعام ١٩٧٧ التي نصت على: "يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو إقتناء سلاح جديد أو أداة للحرب أو إتباع إسلوب للحرب أن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق (البروتوكول) أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف

السامي المتعاقد". فبموجب هذه المادة إن الأنشطة الإلكترونية بوجه عام و الهجمات السيبرانية بشكل خاص سواءاً كانت طريقة أو وسيلة قتالية يجب أن لاتخالف قواعد القانون الدولي بأي شكل من الأشكال .

المطلب الثاني: تكييف الهجمات السيبرانية في القانون الدولي

إن تكييف الهجمات السيبرانية، بالذات بعد تنامي إستخدام شبكة المعلومات والإتصالات في شتى المجالات وتنوع أشكال التهديدات الناجمة عنها وصورها بشكل مطرد، يشكل تحدياً كبيراً يواجهه التنظيم الدولي المعاصر[٣٥].

وعليه فلابد من تكييف الهجمات السيبرانية في ظل كل من قانون الحرب (Jus ad Bellum) الذي يوجد بين ثنايا القانون الدولي العام، و القانون الدولي الإنساني أو القانون في الحرب (Jus in Bello)، ذلك لأن القانون الدولي يميز بين أسباب النزاع المسلح والنزاع المسلح نفسه وهذا التمييز يشكل عنصراً حاسماً في كفالة إحترام كلا القانونين[٣٦]، فالغاية من القانون الدولي الإنساني أو القانون في الحرب هي حماية ضحايا النزاعات المسلحة بغض النظر عن إنتماءهم لأطراف النزاع أو مدى شرعية النزاع . فهو يقتصر على تنظيم جوانب النزاع ذات الأهمية الإنسانية و تسري أحكامه على الأطراف المتحاربة بغض النظر عن مدى عدالة القضية التي يدافع عنها هذا الطرف أو ذاك، بخلاف قانون الحرب الذي يبحث في مدى شرعية النزاع المسلح و يسعى الى تقييد اللجوء الى القوة فيما بين الدول . وهذا هو السبب في أهمية التمييز وإستقلال قانون الحرب عن القانون في الحرب[٣٧].

لا شك بأن ظهور الهجمات السيبرانية وتغيير نمط النزاع المسلح ومجاله وأشخاصه وآثاره يثير كثيراً من التساؤلات: هل الهجوم السيبراني يعد استخداماً للقوة؟، وهل يخرق سيادة الدول؟، هل تنطبق عليه مبادئ القانون الدولي الإنساني؟. و هذا ما سنحاول الإجابة عنه .

الفرع الأول: تكييف الهجمات السيبرانية في ظل قانون الحرب(Jus ad Bellum)

إن قانون الحرب يشير إلى الظروف التي يمكن للدول فيها اللجوء إلى النزاع المسلح أو إستخدام القوة المسلحة بشكل عام، أي بعبارة اخرى يبحث في مشروعية اللجوء إلى استخدام القوة المسلحة[٣٨]. ومن أجل بناء عالم يسوده السلام، أكد ميثاق الأمم المتحدة على تسوية النزاعات بالطرق السلمية و حظر أعمال العدوان ومنع التهديد بإستخدام القوة ضد أي دولة [٣٩].

إن الهجمات السيبرانية تشكل تهديداً للمبادئ الرئيسية في القانون الدولي كإحترام سيادة الدول، لما فيها من اختراق لمعلومات أمنية وعسكرية تصنف بالسرية، و تقوض واجباً أساسيا، وهو الإمتناع عن إستخدام أو التهديد بإستخدام القوة نظراً إلى أضرارها البالغة على سير عمل الحكومة والخدمات في الدولة التي تتعرض لمثل هكذا هجمات[٤٠].

أولا: مبدأ السيادة

تعد فكرة السيادة والإعتراف بها للدول من المبادئ المتفق عليها في ميثاق الأمم المتحدة والإتفاقيات الدولية التي تصب في هذا الصدد. إذ أشارت الفقرة الأولى من المادة الثانية من ميثاق الأمم المتحدة إلى مبدأ المساواة في السيادة بين جميع أعضائها بالنص: " تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها"[٤١].

إن السيادة بمعناها التقليدي تتضمن حق الدولة في السيطرة على إقليمها وتمتعها بمباشرة سلطاتها عليه، و إنها تمثل إنفراد الدولة بإصدار القرارات السياسية والقدرة على الإحتكار الشرعي لأدوات القمع في الداخل ورفض الإمتثال لأي سلطة أجنبية أخرى[٤٢].

ومن التحديات الراهنة أمام سيادة الدولة ونطاقها، ظهور الهجمات السيبرانية، فالتغييرات التكنولوجية الهائلة وتطورات إستخدام الحاسوب وشبكات الإتصال التي نعيشها في الوقت الحاضر والتي لا تعترف بالحدود الجغرافية، خلقت فضاءاً جديداً إلى جانب البر والبحر والجو والفضاء الخارجي، وهو الفضاء السيبراني (Cyber-Space)[٤٣].

إن الفضاء السيبراني يختلف عن العالم المادي الطبيعي من عدة جهات أهمها : إنعدام جغرافية المكان الطبيعي وهو بمثابة فسحة جديدة هرعت إليها الحركة العلمية والثقافية المعاصرة وصولاً إلى اتخاذها صورتين هما : الجريمة والهجمات التي تمس سيادة الدولة المستهدفة[٤٤]. وأصبح هذا الفضاء هو المسرح الحقيقي للهجمات السيبرانية الذي باتت الأطراف الدولية تتنازع وتتسابق على إستغلاله لمصلحتها والقيام بتطوير قدراتها الهجومية والدفاعية ضمن شكل جديد من أشكال سباقات التسلح[٤٥].

وفي ظل هذا التغيير التكنولوجي، فقد تغير المفهوم التقليدي للسيادة من خلال ظهور مفاهيم جديدة منها ما يعرف بالسيادة الرقمية التي تعرف بأنها "بسط الدولة لسيطرتها و ولايتها القضائية على الفضاء الرقمي المتمثل بالإنترنت الذي يجتاز حدود الدولة وينشيء مجموعة أشخاص إفتراضية ضمن شبكات إلكترونية ما وراء أي إنتماء وطني"[٤٦]. وهنا ظهر التحدي الحقيقي، إذ لا تستطيع الدولة فرض سيطرتها على مواطنيها في الفضاء السيبراني عن طريق الجنسية مثلاً، كما لا يقتصر الفضاء السيبراني على الإحاطة بالمفاهيم الجغرافية التقليدية بل يمتد ليشمل ظاهرة تغييب الهوية الوطنية[٤٧].

إن مستخدمي شبكات الكمبيوتر والإنترنت، أي الأفراد الذين يكونون الفضاء السيبراني ينتمون إلى مجتمعات سياسية متعددة وفي حال إرتكاب جريمة ما ضمن هذا الفضاء وقيام الدولة بتتبع مصدر الجريمة، فقد تنتهك في سبيل ذلك مفهوم السيادة الوطنية إذ قد يكون مصدر الجريمة ينتمي أو واقع ضمن نطاق سيادة دولة أخرى.

وبناءاً على ما سبق فيمكن القول بأن سيادة الدولة التقليدية ومقوماتها بدأت تتقلص بوجود وسائل الإتصال الإلكترونية التي تجعل الحدود الإقليمية للدول

والإنتماءات الوطنية تتضاءل شيئا فشيئا، مما تثير التساؤل بشأن نطاق سيادة الدولة في الفضاء السيبراني(٤٨).

إن إضمحلال الحدود الجغرافية في الفضاء السيبراني و المخاطر الناشئة عنه حدت بالدول لتشرع بمعالجة مشاكل السيادة ، لتلافي المخاطر المستقبلية نتيجة إستخدام الفضاء السيبراني ، سواء على الصعيد الوطني أم الدولي. فقامت أغلبيتها بتطوير تشريعاتها الوطنية لإستيعاب الجرائم التي تحدث في نطاق إقليمها و قامت بالتنسيق مع الدول الأخرى عن طريق إبرام إتفاقيات تعنى بتنظيم الجرائم السيبرانية وحل مشكلة السيادة من خلال الإتفاق على آليات تتبع مصادر الجريمة والقوانين واجبة الإتباع في حال حدوثها كالتوصية الصادرة من مجلس أوروبا بشأن المشاكل الإجرائية المرتبطة بتكنولوجيا المعلومات(٤٩)، واتفاقية بودابست عام ٢٠٠١(٥٠)، وبروتوكول ستراسبورغ عام ٢٠٠٣(٥١)، والإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠(٥٢).

وعلى العموم فإن مبدأ السيادة الإقليمية ينطبق على الفضاء السيبراني ويشمل البنية التحتية الإلكترونية سواء كانت على إقليم الدولة ام مياهها الداخلية ام بحرها الإقليمي ام حتى مياهها الأرخبيلية، فيحق للدولة أن تمارس الرقابة على أنشطة البنية التحتية السيبرانية، كنظم الحواسيب و شبكات الإتصال و المعلوماتية و قطاعات الطاقة و النقل و .... في تلك المناطق ، مع الأخذ بنظر الإعتبار إن ممارسة تلك السيادة يمكن أن تنظم وفقا للقواعد العرفية أو المقننة للقانون الدولي(٥٣).

وقد ذهب الخبراء في حلف الشمال الأطلسي إلى أبعد من ذلك حيث أكدوا أن على الدول واجب منع إستخدام البنى التحتية السيبرانية الواقعة في إقليمها أو التي تخضع لسيطرتها الكاملة (Overall Control) في نشاطات تمس الحقوق السيادية للدول الأخرى(٥٤).

و من خلال ما تقدم يمكن القول إن سيادة الدولة على البنى التحتية السيبرانية لا تقتصر على تلك الواقعة أو المشيدة على إقليم الدولة ، بل تمتد إلى كل البنى التحتية السيبرانية التي تخضع لسيطرتها بشكل كامل وإن كانت في إقليم دولة أخرى(٥٥).

و في ضوء ما سبق، فإن الهجمات السيبرانية التي توجه من قبل دولة معينة ضد البنى التحتية السيبرانية التابعة لدولة أخرى ، يمكن أن تمثل خرقاً لسيادة دولة الإقليم خاصة إذا تسببت تلك الهجمات بإحداث آثار مدمرة(٥٦).

ثانيا: مبدأ حظر إستخدام القوة أو التهديد بإستخدامها

إن المادة الثانية من ميثاق الأمم المتحدة تنص في الفقرة الرابعة منها على: "يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد بإستخدام القوة أو إستخدامها ضد سلامة الأراضي أو الإستقلال السياسي لأية دولة، أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة(٥٧). ويتمم هذا الحظر بقاعدة عدم التدخل الواردة في القانون الدولي العرفي التي تحظر الدول من التدخل في الشؤون الداخلية للدول الأخرى(٥٨). كما أكدت محكمة العدل الدولية (ICJ) في قضية الانشطة العسكرية

وشبه العسكرية (نيكاراغوا ضد الولايات المتحدة) بأنه متى ما إتخذ التدخل شكل إستخدام أو التهديد بإستخدام القوة فإن قاعدة عدم التدخل الواردة في القانون الدولي العرفي تتطابق مع المادة (٢ / رابعاً) من ميثاق الأمم المتحدة[٥٩].

إن حظر استخدام القوة الوارد في المادة (٢/ رابعاً) ليس مطلقاً بل يخضع لإستثناءين: الإستثناء الأول هو في موضوع الأمن و السلم الدوليين الوارد في المادة (٣٩) من ميثاق الأمم المتحدة التي تمنح السلطة لمجلس الأمن لتحديد وجود أي تهديد أو خرق للسلم أو عمل من أعمال العدوان، ومن ثم له أن يقرر الإجراءات واجبة الإتخاذ للحفاظ على أو إستعادة السلم والأمن الدوليين[٦٠]، و ينص الميثاق على سلطة مجلس الأمن في إتخاذ التدابير التي لا تتضمن إستخدام القوة المسلحة[٦١]، أو له العمل عن طريق القوات البرية والبحرية والجوية[٦٢].

أما الإستثناء الثاني على المادة (٢/ رابعاً) فهو بشأن حق الدفاع الشرعي الذي ورد في المادة (٥١) من ميثاق الأمم المتحدة، حيث نصت هذه المادة على: "ليس في هذا الميثاق ما يضعف أو ينقص من الحق الطبيعي للدول فرادى أو جماعات في الدفاع عن أنفسهم إذا إعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة، و ذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين"[٦٣]. إن هذه المادة تشترط على الدول لإستخدام حقها في الدفاع الشرعي أن تكون قد تعرضت لإعتداء مسلح، ومن ثم إن الأشكال الأخرى من إستخدام القوة التي لا تكون بمثابة هجوم مسلح لا تعطي الحق في الدفاع الشرعي.

و بموجب هذه الإستثناءات، يعتمد جواز إستخدام القوة المسلحة على وقوع العدوان، وقد جاء تعريف العدوان في قرار صادر من الجمعية العامة للأمم المتحدة بأنه: "إستخدام القوة المسلحة بواسطة دولة ضد السيادة او السلامة الإقليمية أو الإستقلال السياسي لدولة أخرى أو بأي شكل آخر لا يتفق مع ميثاق الأمم المتحدة"[٦٤].

و مما تقدم قد يتبادر الى الذهن السؤال الآتي : هل تشكل الهجمات السيبرانية هجوماً مسلحاً أم شكل آخر من أشكال القوة؟، وهل تعرض دولة ما لهجوم سيبراني يمنحها الحق في الدفاع الشرعي؟.

للإجابة عن هذه التساؤلات لابد من التطرق الى النظريات الرئيسة التي برزت لتحديد متى يمكن عد الهجوم السيبراني هجوماً مسلحاً ومن ثم يرتب الحق في الدفاع الشرعي، منها النهج القائم على الوسيلة (Instrument-Based Approach) حيث تبنى أصحاب هذا النهج معيار الوسيلة المستخدمة في الهجوم وبموجب هذه النظرية، إن الهجوم السيبراني بمفرده ، لن ينشئ لمفهوم هجوم مسلح يستوجب حق الدفاع الشرعي الوارد في المادة (٥١) من ميثاق الأمم المتحدة لأنه "يفتقر الى الخصائص الفيزيائية المرتبطة بالإكراه العسكري". و بعبارة أخرى لأنه بشكل عام لا يحتوي طاقة حركية (Kinetic) مثل ما هو معروف في الأسلحة التقليدية[٦٥]. و ما يدعم هذه النظرية تعريف العدوان الوارد في قرار صادر عن الجمعية العامة للأمم المتحدة حيث أدرج في الفقرة الثالثة منه ، عدداً من الأعمال التي من شأنها أن تشكل "العدوان، بموجب المادة (٣٩) من الميثاق"[٦٦]، وكل

تلك الأعمال وإن جاءت على سبيل المثال وليس الحصر، تتضمن إستخدام الأسلحة التقليدية أو القوة العسكرية ، و مع ذلك يحق لمجلس الأمن أن يعتبر فعل ما عدواناً ولو لم يرد شكل هذا العدوان في الفقرة الثالثة من هذا القرار[٦٧].إن هذه النظرية وإن كانت سهلة التطبيق نظراً لسهولة تحديد الأسلحة والقوة العسكرية، إلا إنها تتغاضى عن الهجمات السيبرانية ذات القدرة البالغة على إحداث الأضرار من دون إستخدام الأسلحة العسكرية التقليدية[٦٨].

أما بموجب النهج القائم على الأهداف (Target-Based Approach) فيكفي أن يستهدف الهجوم السيبراني نظاماً الكترونياً مهماً للغاية، لكي يصنف هجوماً مسلحاً و يركز أصحاب هذه النظرية على طبيعة الهدف الذي يتم إستهدافه، فالهجوم السيبراني يحتاج الى إختراق نظام رئيسي، على سبيل المثال البنى التحتية الوطنية الحرجة للدولة كالنظم المصرفية، لتسويغ الردود العسكرية التقليدية في مواجهته والتي يمكن أن تشعل حرباً تقليدية (Conventional War)[٦٩]. وقد إنتقدت هذه النظرية بسبب تجاهلها لمفهوم البنى التحتية الحرجة المتعددة الأغراض للدولة في العصر الراهن ، فضلاً عن جسامة الهجوم السيبراني و آثاره[٧٠].

و هناك النهج القائم على الآثار (Effects-Based Approach) الذي يعد نهجاً وسطاً بين النهج القائم على الوسيلة و النهج القائم على الأهداف. إذ يصنف أصحاب هذه النظرية الهجوم السيبراني كهجوم مسلح على أساس خطورة آثاره[٧١]. وقد ذهب بعض الفقهاء المؤيدين لهذه النظرية الى تحديد العوامل التي يمكن القياس عليها لتصنيف الهجوم السيبراني كهجوم مسلح ومن هذه العوامل الخطورة ، الفورية و المباشرة والقابلة للقياس[٧٢].كما يرى أصحاب هذه النظرية إن كل نشاط مشبوه يمكن معاقبته على وفق آثاره على الدول الأخرى[٧٣].و بموجب هذه النظرية فإن الهجوم السيبراني على سبيل المثال ضد نظام مراقبة الملاحة الجوية، والتسبب بحوادث الطائرات، سيعد هجوماً مسلحاً لأنه من المتوقع أن هجوماً كهذا سيتسبب في خسائر كبيرة سواء في الأرواح ام الأموال. مما سبق يمكن القول: إن هذا الإتجاه وإن كان هو الإتجاه الأكثر أهمية وقبولاً من النظريات السابقة ، إلا أنه لا ينطبق إلا على مجموعة صغيرة من الهجمات السيبرانية الضارة، أي تلك التي لها آثار تماثل آثار الهجوم بإستخدام أسلحة تقليدية او أسلحة الدمار الشامل[٧٤].

وتأسيساً على ما تقدم يمكن القول إن الهجمات السيبرانية متى ما كانت آثارها شبيهة بآثار الهجوم المسلح التقليدي من ناحية الإصابات الجسدية والأضرار المادية فإنها تكيف كإستخدام للقوة المسلحة المعروفة ، وبالتالي للدولة المتضررة اللجوء الى إستخدام حقها في الدفاع عن النفس[٧٥].

من ناحية أخرى إن المادة (٢/ رابعاً) لم تحظر إستخدام القوة المسلحة فقط، بل حظرت التهديد بإستخدامها ضد الدول الأخرى وقد تم تعريف التهديد بإستخدام القوة بأنه: "التهديد الصريح أو الضمني، شفاهاً أو عملاً ، بإستخدام غير الشرعي

للقوات المسلحة ضد دولة أو عدة دول والذي تحقيقه يتعلق بإرادة الدولة التي قامت بعمل التهديد"(٧٦).

وبناءاً على ما نصت عليه محكمة العدل الدولية في رأيها الإستشاري بشأن شرعية استخدام الأسلحة النووية او التهديد باستخدامها في الفقرة ال٤٧ بأن (مفهوما "التهديد" بالقوة و "إستعمال" القوة وفقا للفقرة ٤ من المادة ٢ من ميثاق الأمم المتحدة متلازمان من حيث إنه إذا كان إستعمال القوة في حالة ما غير مشروع _لأي سبب من الأسباب_ فإن التهديد بإستعمال هذه القوة هو أيضا غير مشروع)(٧٧). فبالتالي إن التهديد بإستخدام الهجوم السيبراني يكون مرتبطاً في شرعيته بمدى شرعية الهجوم السيبراني ذاته.

و الجدير بالذكر إن الهجمات السيبرانية التي ترقى الى مستوى الهجوم المسلح، وإن كانت تسوغ حق الدفاع عن النفس، إلا أن هذا الحق ليس مطلقاً. فإستخدام الدولة للقوة المسلحة رداً على الهجوم السيبراني، يجب أن يتفق ليس فقط مع ميثاق الأمم المتحدة بل وقواعد القانون الدولي العرفي، وما تضمنته مبادئ استخدام القوة المسلحة كمبدأي الضرورة العسكرية ومبدأ التناسب في استخدام القوة المسلحة أيضاً(٧٨).

إن السؤال الذي يثار هنا هو، إذا لم تكن الهجمات السيبرانية ذات آثار جسيمة تبلغ مستوى النزاع المسلح، فهل يمكن القول بأنها غير منظمة قانونيا؟ وكيف للدولة المتضررة الرد على مثل هذه الهجمات؟

للإجابة لابد من القول بأن الهجمات السيبرانية التي لا يمكن عدُ إستخدامها للقوة محظوراً بموجب المادة (٢/ رابعاً) من ميثاق الأمم المتحدة، يمكن عدُها شبيهة بأعمال الضغط السياسي والإقتصادي، وفي هذه الحالة تخرق قاعدة (عدم التدخل) الواردة في القانون الدولي العرفي(٧٩). وعلى هذه الشاكلة يمكن القول: إن المادة (٢ رابعاً) من ميثاق الأمم المتحدة تشير الى إستخدام القوة المسلحة ، إلا إن مبدأ (عدم التدخل) ينطبق على الأشكال الأخرى لإستخدام القوة(٨٠).

الفرع الثاني: تكييف الهجمات السيبرانية في ظل القانون في الحرب (Jus in Bello)

على الرغم من أن الهجوم السيبراني القائم بذاته لا يشكل نزاعاً مسلحاً، إلا إن الهجمات السيبرانية قد يتم إستخدامها أثناء النزاعات المسلحة للرد على إستفزازات تقليدية أو لتمهيد الطريق لهجوم تقليدي بهدف تحقيق التفوق والميزة العسكرية(٨١).

إن توظيف الهجمات السيبرانية في النزاع المسلح كما جاء في تقرير اللجنة الدولية للصليب الأحمر عام ٢٠١١ يجب أن يتوافق مع جميع مبادئ القانون الدولي الإنساني و قواعده كما هو الحال مع أي سلاح أو وسيلة أو إسلوب حرب آخر، جديداً كان أم قديماً(٨٢).

وما يؤيد ذلك ما أشارت اليه محكمة العدل الدولية إن :" مبادئ وقواعد القانون الدولي الإنساني المنطبق في النزاع المسلح، تنطبق على "جميع أشكال الحروب وعلى جميع أنواع الأسلحة.. بما في ذلك تلك المستقبلية"(٨٣).

وبناء على ذلك فإن القانون الدولي الإنساني أو القانون في الحرب (Jus in Bello) ينطبق على الهجمات السيبرانية التي تحدث في أثناء نزاع مسلح دائر.

أولا: الحالات المقننة في القانون الدولي الإنساني

إن التحديات الجديدة أمام القانون الدولي الإنساني كالهجمات السيبرانية تثير مسألة مدى إنطباق مبادئ هذا القانون عليها كمبدأ الضرورة العسكرية والتناسب في إستخدام القوة والتمييز بين المدنيين و المقاتلين.

إن مبدأ الضرورة العسكرية يتعلق بميزة عسكرية محددة يمكن تحقيقها من عمل عدائي خاص وعلى صعيد القانون الدولي فقد تمت الإشارة إلى مبدأ الضرورة العسكرية في صكوك دولية عدة منها ديباجة إعلان سان بيترسبورغ عام ١٩٦٨، الذي نصت على "... أن الهدف المشروع الوحيد الذي يجب أن تسعى إليه الدول في أثناء الحرب هو إضعاف القوات العسكرية للعدو..."[٨٤]. وقد ذهبت لجنة القانون الدولي بمناسبة تعرضها إلى المشروع الخاص بالمسؤولية الدولية بالقول: "لابد من التذكير بعدم جواز اللجوء إلى الضرورة العسكرية ، إلا إذا لم تستطع الدولة بلوغ أهدافها العسكرية المشروعة إلا بالقيام بعمل طارئ وضروري لتحقيق ذلك الهدف حماية لمصالح الدولة العليا"[٨٥].

إستناداً إلى ما سبق يمكن القول إن اللجوء الى الهجمات السيبرانية يجب أن يكون ضرورياً لتحقيق الهدف العسكري المشروع ، وأما مسألة تحديد الأهداف والمنشآت العسكرية في الفضاء السيبراني فتثير تحدياً واسعاً أمام المجتمع الدولي ، وذلك لأن المنشآت التي تقدم خدمة للجهد العسكري هي في الوقت نفسه قد تخدم القطاع المدني. إن عدم تحديد معايير منظمة لإستخدام الفضاء السيبراني للأغراض العسكرية الهجومية سيعني إمكانية اللجوء لإستخدامها بداعي الضرورة العسكرية[٨٦]. وقد أشار إلى هذا التحدي ريكس هيوز (Rex Hughes) مدير شبكة الإبتكار السايبري في جامعة كامبردج بالقول: "إن الهجمات الرقمية تنشئ تحدياً واضحاً أمام تطبيق مبدأ الضرورة العسكرية ولحل هذه المعضلة لابد من تضافر الجهود بين خبراء القانون الدولي ومهندسي الصناعات الإلكترونية لتحديد ما يمكن أن يوصف بهدف..."[٨٧].

أما مبدأ التناسب في إستخدام القوة في النزاع المسلح قد أكدت عدة صكوك دولية على واجب مراعاته، منها ما ورد في البروتوكول الإضافي الأول لعام ١٩٧٧ في الفقرة (٥/ب) من المادة (٥١) إذ نصت بأنه : "الهجوم الذي يتوقع منه إحداث خسائر عرضية في أرواح المدنيين، إصابة المدنيين، الإضرار بالأعيان المدنية أو مزيجاً منها، الذي سيكون مفرطاً فيما يتعلق بالميزة العسكرية المباشرة والملموسة المرتقبة"[٨٨].

أما بشأن الهجمات السيبرانية فنظراً إلى طبيعة الضرر الذي تحدثه هذه الهجمات، فإن تحقيق مبدأ التناسب فيها يشكل تحدياً فريداً من نوعه أمام التنظيم الدولي وذلك لأن آثار الهجوم السيبراني عادة ما تكون غير مباشرة[٨٩]. على سبيل المثال أن الهجوم السيبراني الذي يوقف تدفق المعلومات عبر الإنترنت قد يبدو مجرد إزعاج في بادئ الأمر، إلا إن ذلك سيؤدي إلى شل قدرة المستشفيات على نقل المعلومات الحيوية، ومن ثم يؤدي إلى خسائر بالأرواح وإصابات بالغة[٩٠]. وهذا ما أيده هيوز حيث ذهب بالقول: "إذا تم توجيه هجمات سيبرانية ضد بنى تحتية ثنائية الإستعمال (مدنية-عسكرية) وعن بعد فلا

يبدو أن الميزة العسكرية ستكون واضحة، ما يجعل من تطبيق مبدأ التناسب في أثناء الهجمات السيبرانية أمراً في غاية الصعوبة"[٩١].

إن تحقيق التناسب في الهجمات السيبرانية قد يكون مستحيلاً، وذلك لأن تكنولوجيا المعلومات والإتصالات غير متساوية في الدول ، ومن ثم قد تكون الدولة الضحية غير متطورة من ناحية تكنولوجيا الهجوم السيبراني لرد الهجمات السيبرانية الموجهة ضدها[٩٢]. و إن تطبيق مبدأ التناسب يتطلب توقع النتائج المحتملة للنشاط العدائي ، وفيما يتعلق بالهجمات السيبرانية و الغموض الذي يكتنف نوع آثار هذه الهجمات و شدتها نتيجة اللامحدودية التي يتمتع بها العقل البشري فإن توقع النتائج المحتملة لهذه الهجمات يجعل تطبيق هذا المبدأ يتسم بصعوبة بالغة بالنسبة للقادة العسكريين الذي عليهم في سياق الهجمات السيبرانية مواجهة المزيد من الشكوك والغموض بشأن شرعية الهجمات التي سينفذونها[٩٣].

أما مبدأ التمييز بين المدنيين و المقاتلين الذي يتطلب من أطراف النزاع التمييز بين الأشخاص المدنيين والمقاتلين و توجيه الهجمات للأهداف العسكرية دون المدنية، يقدم تحدياً آخر أمام القانون الدولي. فبموجب هذا المبدأ على القادة العسكريين إستخدام الوسائل التي بإمكانها الاستهداف الدقيق (غير عشوائية الأثر)، للتمييز بين السكان المدنيين والمقاتلين، وأيضاً بين الأعيان المدنية والأهداف العسكرية"[٩٤]. أما في نطاق الهجمات السيبرانية و طبقا لهذا المبدأ فيحظر على أطراف النزاع شن هجمات توجه ضد أهداف غير عسكرية يقصد بها أو يتوقع منها أن تتسبب بالموت أو الإصابة أو التلف أو الدمار.

إن تطبيق مبدأ التمييز على الهجمات السيبرانية يتسم بكثير من التعقيد، وذلك لتشابك الإستخدام المدني والعسكري لنفس الشبكات حيث أن خمسة وتسعون بالمئة (٩٥٪) من الإتصالات العسكرية تستخدم الشبكات المدنية في بعض المستويات. و بموجب الفهم التقليدي للأعيان ذات الإستخدام المزدوج(Duble-Uses) فإنه متى ما إستخدمت عيناً معينة لأغراض مدنية وعسكرية على حدٍ سواء فإن تلك العين تصبح هدفاً عسكرياً مشروعاً، إذا أسهمت مساهمة فعالة في العمل العسكري أو تحقق تدميرها ميزة عسكرية أكيدة بشرط أن تراعي مبدأ التناسب بشأن الأضرار التي تلحق بالمدنيين[٩٥]. أما في الفضاء السيبراني فإن كثيراً من الأعيان التي تشكل بنيته الأساسية هي مزدوجة الإستخدام، ما يجعل منها أهدافاً عسكرية جذابة[٩٦] وغير مشمولة بالحماية سواء من الهجمات الحركية ام السيبرانية، إلا إن ذلك يبقى محكوماً بحظر الهجمات العشوائية وبقواعد التناسب و اتخاذ الإحتياطات المستطاعة في أثناء الهجوم، ولأن الشبكات الالكترونية المدنية والعسكرية مترابطة إلى حد بعيد، فيجب توقع الضرر المدني العرضي في معظم الحالات[٩٧].

أما التحدي الأصعب في تطبيق مبدأ التمييز على الهجمات السيبرانية ، فهو تمييز المدنيين عن المقاتلين، وذلك لعدة أسباب منها، إن الهجوم السيبراني غالباً ما يتم عن

طريق أشخاص قد يبعدون عن محل الهجوم مسافات قد تتجاوز مئات الأميال، وهذا ما يجعل التمييز بين المقاتل والمدني صعباً للغاية إن لم يكن مستحيلاً[٩٨].

و قد تقوم الدول بتقويض مبدأ التمييز من خلال إستخدامها المدنيين في تنفيذ الهجمات السيبرانية، حيث بفعلها هذا تضع أولئك المدنيين خارج نطاق الحماية التي يتمتعون بها بموجب القواعد الدولية، وذلك لمشاركتهم في الأعمال القتالية[٩٩]

ثانيا:الحالات غير المقننة في القانون الدولي الإنساني(مبدأ مارتنز)

جاءت تسمية (مارتنز) نسبة إلى الدبلوماسي الروسي فيدور فيودوفج مارتنز أحد مندوبي روسيا في مؤتمر السلام عام ١٨٩٩، الذي صرح فيه: "في الحالات غير المشمولة بالأحكام، يظل السكان المتحاربون تحت حماية وسلطان مبادئ قانون الأمم كما جاءت من تقاليد إستقر عليها بين الشعوب المتمدنة وقوانين الإنسانية ومقتضيات الضمير العام"[١٠٠]. وقد ورد هذا الشرط في مقدمة إتفاقيات لاهاي لعامي ١٨٩٩ و ١٩٠٧ المتعلقة بقواعد وأعراف الحرب البرية وكذلك في اتفاقيات جنيف لعام ١٩٤٩كما تم إدراجها في البروتوكول الإضافي الأول لعام ١٩٧٧، حيث نصت الفقرة الثانية من المادة الاولى بأنه: "يظل المدنيون والمقاتلون في الحالات التي لا ينص عليها في هذا البروتوكول، أو أي اتفاق دولي آخر، تحت حماية وسلطان مبادئ القانون الدولي، كما إستقر عليه العرف ومبادئ الإنسانية وما يمليه الضمير العام[١٠١].أما في سياق الهجمات السيبرانية فيمكن الإستناد إلى ما أورده القاضي شهاب الدين في الرأي الإستشاري الصادر عن محكمة العدل الدولية عام ١٩٩٦ بخصوص شرعية التهديد وإستعمال الأسلحة النووية حيث أكد على: "يمنح شرط مارتنز سلطة معالجة مبادئ القانون الإنساني وما يمليه الضمير العام بوصفهما مبادئ من القانون الدولي، تاركاً المحتوى الدقيق للمعيار الذي ستلزمه مبادئ القانون الدولي على ضوء الظروف المتغيرة، بما في ذلك التغيرات في وسائل الحرب ومستويات مظهر المجتمع الدولي وتسامحه"[١٠٢].

كما ذهبت المحكمة في رأيها الإستشاري بخصوص شرعية التهديد وإستعمال الأسلحة النووية بأن شرط مارتنز "أثبت أنه وسيلة فعالة لمواجهة التطور السريع في التكنولوجيا العسكرية"[١٠٣]. وعلى هذا الأساس أكدت المحكمة أن المبادئ الأساسية للقانون الإنساني تظل منطبقة على جميع الأسلحة الجديدة بما فيها الأسلحة النووية، وذكرت إنه لا توجد دولة تجادل في ذلك[١٠٤].

مما سبق يتبين إن عدم وجود قواعد دولية محددة -عرفية كانت أم تعاهدية – تنظم الهجمات السيبرانية، لا يعني الإقرار ضمناً بجواز اللجوء إليها، لأنها تتنافى بطبيعتها مع القوانين الإنسانية وما يمليه الضمير العام العالمي في حال إنها استهدفت منشآت تحوي قوى خطرة كالمحطات النووية وأنابيب النفط أو أعيان مدنية ضرورية لبقاء الإنسان كشبكات الكهرباء والمياه[١٠٥].

خلاصة القول إن شرط مارتنز يعد صمام الأمان الذي يمنع الدول وغيرها من الأطراف المتنازعة من إستخدام و إستحداث وسائل قتال جديدة كما يقطع الطريق أمام الدول للتهرب من المسؤولية بحجة عدم وجود قواعد قانونية تحكم الوسائل والأساليب

الجديدة التي لم يتطرق إليها القانون الدولي الإنساني، و هو ما يمكن التعويل عليه في تحريك المسؤولية الدولية الناشئة عن الهجمات السيبرانية ، لسد الذريعة بعدم وجود أحكام دولية صريحة تحظر إستخدامها.

الخاتمة

خلصنا في هذه الدراسة الى إن الهجمات السيبرانية هي واحدة من أهم التحديات المعاصرة التي تواجه المجتمع الدولي، لما لها من تداعيات على الأمن القومي للدول و تهديدها للسلم و الأمن الدوليين. و في أثناء البحث القانوني عن مفهوم هذه الهجمات و موقعها من التنظيم الدولي المعاصر توصلنا الى عدة نتائج و توصيات و على النحو التالي:

النتائج:

١- إن الهجمات السيبرانية مازالت من المفاهيم الحديثة التي لا يوجد إتفاق دولي بشأن تعريفها مما يؤدي الى صعوبة تكييفها و تحديد المسؤولية الدولية عنها.

٢- تكمن الميزة النسبية للهجمات السيبرانية في إنخفاض تكاليفها و سهولة اللجوء اليها إذ لا تتطلب حشوداً من المقاتلين العسكريين و الآلاف من الأسلحة والوسائل كالنزاعات المسلحة التقليدية، بل يكفي لتنفيذها شخص أو مجموعة صغيرة ممن لديهم الخبرة و المهارة في التكنولوجيا السيبرانية وثغرات البرامج والأنظمة الكمبيوترية لإستخدامها ضد دولة أو دول أخرى، إلا إن هذه الميزة تتحول الى مصدر قلق كبير إذا ما نظرنا إلى آثار هذه الهجمات و تبعاتها على السكان المدنيين والبيئة فيما لو تم تنفيذها على منشأة نووية أو مصادر الطاقة كشبكة الكهرباء و المياه.

٣- فيما يخص الهجمات السيبرانية التي تحدث في أثناء النزاع المسلح التقليدي فقد أجمع الفقهاء الدوليين على خضوعها للقانون الدولي الإنساني.

٤- إن التحدي الأكبر في تكييف الهجمات السيبرانية هو تلك الهجمات التي تحدث في وقت السلم و مدى إمكانية عدها هجوما مسلحا يثير حق الدفاع الشرعي، و متى تعد خرقا لمبدأ "عدم التدخل" الذي يسمح فقط بإستخدام التدابير المضادة و الطرق السلمية الأخرى في مواجهتها .

٥- تعد العلاقة بين القانون والتكنولوجيا علاقة تبادلية، فالتطورات التكنولوجية المختلفة تفترض مواكبة التشريعات القانونية لها، سواء على الصعيد الداخلي للدولة أو على الصعيد الدولي، إلا إن الأنشطة السيبرانية (خاصة الهجوم السيبراني) تفتقد الى الأطر القانونية الصارمة للتعامل معها، والتنظيمات والقوانين الدولية المعاصرة وإن كانت تنطبق على الهجمات السيبرانية إلا إنها لا تغطي كل أشكال وتحديات الهجمات السيبرانية.

٦- إن عملية وضع تنظيم شامل لهذه الظاهرة الخطيرة تتسم بصعوبات شتى وذلك لأن المصالح الدولية للقوى العظمى تقف حجر عثرة أمامها، كالصعوبات التي

واجهت المجتمع الدولي عند وضع إتفاقية بشأن الأسلحة النووية والجدل حول تقييدها أو حظر إستخدامها كلياً .

التوصيات

١- لابد من عقد إتفاقيات دولية بشأن تنظيم هذه الهجمات بشكل تفصيلي وذلك لحماية المجتمع الدولي من العواقب الإنسانية الوخيمة سواء الدموية منها أم المادية أم البيئية .

٢- فصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية وذلك لحماية السكان المدنيين من مخاطر الهجمات السيبرانية.

٣- يتوجب على الدول إتخاذ خطوات جدية لمواجهة الهجمات السيبرانية بإعتماد تدريس الفضاء السيبراني والمخاطر الناشئة عنه،لا سيما على المستوى الدولي، في المؤسسات الأكاديمية

الهوامش

(1) Oona A. Hathaway, Rebecca Crootof , Philip Levitz, Haley Nix, Aileen Nowlan , William Perdue & Julia Spiegel, "The law of Cyber-Attack", California law review, 2012, p.824.

(2)Ibid, p. 824.

(3) K. Saalbach, "Cyber war, Methods and Practice", version 2.0, university of Osnabruck-17 Jun 2014, p.8.

(4) Micheal S. Fuertes, "Cyber warfare, Unjust Actins in a just war" Florida International University, Full 2013, p.1.

(5) Oona Hathaway, op. cit., p.825.

(6) Shanghai Cooperation Agreement, Annex I, p. 203.

(٧) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،مجلة المحقق الحلي للعلوم القانونية و السياسية، جامعة بابل، السنة الثامنة، العدد الرابع، ٢٠١٦، ص٦١٦.

(8)Micheal N.Schmitt. William H.Boothby. Wolff Heintschel Von Heinegg. Thomas C.Wingfield. Eric Talbot Jensen. Seen Whatts. Louise Arimatsu. Genevieve Bernatchez. Penny Cumming. Robin Geiss. Terry D.Gill. Derek Jinks. Jann Kleffner. Nils Melzer & Kenneth Whatkin , "Tallinn Manual on the International Law Applicable to Cyber warfare", Cambridge University Press, First Publishes, 2013, p. 92.

(٩) غازي عبد الرحمن هيان الرشيد،الحماية القانونية من جرائم المعلوماتية (الحاسب و الإنترنت)،إطروحة لنيل درجة الدكتوراه في القانون ،الجامعة الإسلامية في لبنان،كلية الحقوق، ٢٠٠٤، ص ١٠٨.

(10) Debra Little John Shinder, sence of the Cybercrime: computer forensics Handbook, p 16.

(١١) و هي اللجنة الإقتصادية و الإجتماعية لغرب آسيا و هي جزءاً من الأمانة العامة للأمم المتحدة تعمل باشراف المجلس الإقتصادي و الإجتماعي ،تأسست إبتداء بعنوان اللجنة الإقتصادية لغربي آسيا في ٩ آب ١٩٧٣ بموجب قرار المجلس الإقتصادي و الإجتماعي ١٨١٨(د-٥٥)و أعيدت تسميتها من قبل المجلس نفسه بموجب القرار ٦٩/١٩٨٥ الصادر في تموز ١٩٨٥ فأصبحت اللجنة الإقتصادية و الإجتماعية لغربي آسيا و تتخذ بيروت مقرا دائما لها، من أهدافها تحفيز التنمية الإقتصادية و الإجتماعية في الدول الأعضاء و تعزيز التعاون بينهم، و تحقيق التكامل الإقليمي بين المنطقة العربية و المناطق الأخرى . تتألف من ١٨ بلدا عربيا في منطقة غرب آسيا.

(١٢) إرشادات الإسكوا للتشريعات السيبرانية ،مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية ،بيروت ،٢٠١٢،ص ١١٧ .

(١٣) محمد علي قطب ،الجرائم المعلوماتية و طرق مواجهتها، الأكاديمية الملكية للشرطة، البحرين ٢٠١٠، متوفر على الموقع:(أخر زيارة بتاريخ ٢٠١٦/٧/٢١)

http://www.policemc.gov.bh/mcms-store/pdf

(14) Oona Hathaway,op.cit , p.834.

(15) Ibid, p 835.

(١٦) مؤسسة راند أو مؤسسة الأبحاث و التطوير هي منظمة غير ربحية تأسست عام ١٩٤٨ من قبل شركة طائرات دوغلاس لتقديم تحليلات و أبحاث للقوات المسلحة الأمريكية.

(17)Cyber Warfare(2015) available at:

http://www.rand.org/topics/cyberwarfare.htm

(18) Martin C. Libicki ,Cyber deterrence and Cyber war ,Project Air Force, prepared for United States Air Force , 2009, p.170-182.

(١٩) قاسم ترابي، تطور إستراتيجية حلف الشمال الأطلسي في مواجهة الحرب السيبرانية الأسباب و الأبعاد و المكونات، دورية مطالعات راهبردي، السنة ال١٨، العدد الأول، ربيع ٢٠١٥، ص ١٣٩ .

(22) Oona Hathaway ,op .cit ,p.833-841.

(21) Murice Abuert, "The ICRC and the problem of excessively or indiscriminate weapons" Extract print from ICRC, No. 279, Nov-Dec. 1990, p.483, Footnote-18.

(٢٢) على سبيل المثال: -تعديل البرتوكول الثاني الملحق باتفاقية "حظر أو تقييد إستعمال أسلحة تقليدية معينة يمكن إعتبارها مفرطة الضرر أو عشوائية الأثر" عام ١٩٩٦. -إتفاقية أوتاوا عام ١٩٩٧. -إتفاقية حظر الذخائر العقودية عام ٢٠٠٨.

(٢٣) قاسم ترابي، مصدر سابق، ص١٣٨.

(٢٤) توليو ستيف وشمالبرغر توماس، "قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبناء الثقة"، معهد الأمم المتحدة لبحوث نزع السلاح، منشورات الأمم المتحدة، ٢٠٠٣، ص٣٧.

(25) Ingrid Detlar, The Law of War, Cambridge , Cambridge University press ,2003 , p.234.

(٢٦) ينظر احمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦١٨.

(27) Mark Clayton, "Stuxnet malware is weapon out to destroy Iran's Bushehr nuclear plant? The Christian Science Monitor, Sep. 21.2010, at this link: www.Csmonitor.com. U.S.A./2010/0921/Stuxnet-Malware-is....

(28) Robert McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program?: pc word", Sep. 12. 2010, at this link:

www.Sscenter/article/205827/was-stuxnet-built-to-attack-iran's-nuclear-program.html.

(٢٩) عادل عبد الصادق، الفضاء الالكتروني واسلحة الانتشار بين الردع وسباق التسلح، ١٥/مايو/٢٠١٥، مؤتمر حروب الفضاء السيبراني، متوفر على الموقع الالكتروني-الفضاء: (أخر زيارة بتاريخ ٢٠١٦/٧/٢٧)

Http://Seconf.wordpress.com/2015/05/

(30) U. S. Dept's of Def., An assessment of Intgernational Legal Issues in information operation 18 (1999). Available at:

http://www/au/of.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf,reprinted in76 INT'S L. Stud. 459, 483 (2002).

(31) Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schojlberg, "Global Cyber Deterrence views from China, the U.S., Russia, India, and Norway", The East West Institute, printed in the United States,2010 ,p.3.

(32) Nils Melzer, "Cyber warfare and International Law", 1 DEAS for Peace and Security. UNIDIR Researches, 2011, p2.

(٣٣) ينظر احمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦١٨.

(٣٤) مقال منشور بعنوان الحروب الالكترونية بتاريخ ٢٨/مايو/٢٠١٢ على الموقع الالكتروني:(آخر زيارة بتاريخ ٢٠١٦/٨/١٢). http://whitehatssecurity.com/28/05/2012/Cyberwars.

(٣٥) احسان كيان خواه و سعيد علوي وفا، مفهوم الأمن السيبراني، مجموعة مقالات المؤتمر الوطني الأول للفاع السيبراني، طهران/ايران، ٢٠١٢، ص٤.

(٣٦) فرانسوا بونيون، الحرب العادلة وحرب العدوان والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر، مختارات من اعداد عام ٢٠٠٢، ص٣٦-٤١.

(٣٧) اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني (إجابات عن أسئلتك)، ديسمبر ٢٠١٤، ص٨-٩.

(٣٨) اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني (إجابات عن أسئلتك)، مصدر سابق. ص٨.

(٣٩) ميثاق الأمم المتحدة، الفصل الأول، المواد ١-،٢ على الموقع الرسمي:
www.un.org>charter-united-nations

(٤٠) محمد علي رعايت كننده فلاح، الحرب السيبرانية و تهديد الأمن القومي لجمهورية ايران الإسلامية، أطروحة دكتوراه، جامعة آزاد اسلامي،كلية الآداب و العلوم الإنسانية، قم/ايران، ٢٠١٢ ، ص ٧٢-٧٦.

(٤١) ميثاق الأمم المتحدة، الفصل الأول، المواد (٢) ف ١.

(٤٢) محمد طلعت الغنيمي، الوسيط في قانون السلام، منشأة المعارف، الاسكندرية، ١٩٩٣، ص٣١٧.

(٤٣) مصطفى عصام نعوس، سيادة الدولة في الفضاء الإلكتروني ، مجلة الشريعة و القانون ، جامعة الإمارات العربية المتحدة ، كلية القانون ، السنة السادسة و العشرون ، العدد ٥١ ، يوليو ٢٠١٢، ص ١٢٨.

(٤٤) عمر بن يونس، المجتمع المعلوماتي، الدار العربية للموسوعات، بيروت، ٢٠١٠، ص١٣.

(٤٥) روبرت كناكي، حوكمة الإنترنت في عصر إنعدام الأمن الإلكتروني، سلسلة دراسات عالمية، مركز الإمارات للدراسات والبحوث الإستراتيجية، أبو ظبي، العدد ٩٥، ٢٠١١ ، ص١٣.

(٤٦) سراب ثامر احمد، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة من متطلبات نيل درجة الدكتوراه في القانون العام، جامعة النهرين، كلية الحقوق، ٢٠١٥، ص١٠١.

(٤٧) ينظر نبيل علي وفادية حجازي، الفجوة الرقمية رؤية عربية لمجتمع المعرفة، سلسلة عالم المعرفة، العدد ٣١٨، (الكويت، المجلس الوطني للثقافة والفنون والآداب، ٢٠٠٥)، ص١٢.

(٤٨) مصطفى عصام نعوس، مصدر سابق، ص ١٣٦-١٣٩.

(٤٩) التوصية الصادرة عن مجلس أوروبا رقم R(95)13 بتاريخ ١١/سبتمبر ١٩٩٥.

(٥٠) مجلس أوروبا، إتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، مجموعة المعاهدات الاوربية رقم ١٨٥،بودابست، عام ٢٠٠١.

(٥١) البروتوكول الإضافي لإتفاقية الجريمة المعلوماتية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهة الأجانب المرتكبة عبر أنظمة الكمبيوتر، ٢+٨ يناير ٢٠٠٣، على الموقع
http://Conventions.Coe.int/treaty/fr/Treaties/Html/189.htm.

(53) Wolff Heintscble Von Heinegg, Territorial Sovereignty and Neutrality in cyberspace, U. S. Naval war college, 2013 volume 89, p. 128.

(54) Tallinn Manual on the International law applicable to cyber warfare,op.cit , charter.1, section. 1 , Rule. 5.

(1) Tallinn manual on the international law applicable to cyber warfare, op. cit., p.27.

(٥٦) سراب ثامر أحمد، مصدر سابق، ص ١١٨.

(٥٧) ميثاق الأمم المتحدة، المادة ٢ (رابعاً).

(58) General Assembly. Res.37/10, U.N. Doc .A/RES/37/10 (Nov., 15, 1982) – also General Assembly Rec. 25/2625, U.N. Doc .A/RES/25/2625 (Oct. 24, 1970).

(59)ICJ, Military and paramilitary activities in and against Nicaragua (Nicar .v. U.S.), 1986, ICJ. 14, (June 27), para. 209.

(٦٠) ميثاق الأمم المتحدة، المادة ٣٩.

(٦١) المصدر السابق، المادة ٤١.

(٦٢) المصدر السابق، المادة ٤٢.

(٦٣) ميثاق الأمم المتحدة، المادة (٥١).

(64) General Assembly, Res. 3314, U.N. Doc. A/RES/3314, (Dec. 14, 1974).

(65) Michael N. Schmitt, Computer network attack and the use of force in International Law: Thoughts on normative framework, International Review of the Red Cross,No.846, 30/6/2002.

(66) UN.General Assembly.Res. 3314, Dec,14,1974.

(٦٧) بدر محمد هلال ابو هويل، جريمة العدوان في القانون الدولي، دراسة لإستكمال متطلبات النجاح في مساق القانون الدولي، جامعة آل البيت، كلية الدراسات العليا، الأردن، ٢٠١٢، ص١٢.

(68) Oona Hathaway, op. cit., p. 846.

(69) Matthew J. Sklerov, solving the Dilemma of state Responses to cyber Attacks: A Justification for the use of Active Defenses against states who Neglect their Duty to prevent, 201 MIL. L. REV., fall 2009, at 1, 74-75.

(70) Gray Sharp, in Stephanie G. Handler, The new cyber Face of the Battle, Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, vol. 48, 2012, p. 12.

(71) Daniel. B. Silver, Computer Network Attack as a Use of Force Under article 2(4) of United Nations Charter, in computer network attack and international law 73, 2002 , p. 13.

(72) Michael N. Schmitt , Computer Network Attack and the use of Force in International Law, op. cit., p. 914.

(73) Sean P. Kanuck, Recent Development: Information warfare: New Challenges for public International Law, 37 Harvard International Law Journal, l. 272, 290 ,1996.

(74) Oona Hathaway, op. cit., p. 848.

(75) Tallinn manual on the international law applicable to cyber warfare,op.cit.,p. 54.

(76) Marco Roscini , "Threats of Armed Force on contemporary International Law". Netherlands International Law Review, No. 54, 2007, p. 235.

(77) ICJ Nuclear weapons Advisory opinion, legality of threats or use of Nuclear weapons. Advisory opinion, 1996, I.C.J. 226 (8 July) , para 47.

(78) Oona Hathaway, op.cit ,p.849.

(79) General Assembly . A/RES/37/10 , op. cit.

(80) A. Randelzhofer, "Article 2(4)", in: Simma, B. (ed), The Charter of the United Nations: A commentary. Vol. 1, 2002, p. 118.

(٨١) مايكل ن.شميث ، الحرب بواسطة شبكات الإتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) و القانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من أعداد ٢٠٠٢،ص ٩٠-٩٤.

(٨٢) اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، تقرير تشرين الاول/اكتوبر ٢٠١١، متاح على الموقع الرسمي:

www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st international-conference/31-int.conference-ihl-challenges-report-11-5-1-2-en.Pdf.

(83) ICJ Nuclear weapons Advisory opinion, op. cit., para 86.

(٨٤) اللجنة الدولية للصليب الأحمر، "القانون الدولي المتعلق بسير العمليات العسكرية، مجموعة اتفاقيات لاهاي وبعض المعاهدات الأخرى" ، جنيف، ط ثانية، سبتمبر/ايلول ٢٠٠١، ص١٦٩.

(85) UN,"Year book of the International Law commission" vol.II,part 1, 1980, Article 3.

(٨٦) أحمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٠-٦٣١.

(87) Rex Hughes , "A Treaty for cyber space", International Affairs Journal, vol. 86, No. 2, 2010, p. 537.

(٨٨) اللجنة الدولية للصليب الأحمر، "الملحقان" "البروتوكولان الاضافيان إلى اتفاقية جينيف المعقودة في ١٢ آب اغسطس ١٩٤٩"، جنيف، سويسرا، ط٤، ١٩٩٧، ص٤٢.

(٨٩) علي قاسمي و ويكتور بارين جهار بخش، الهجمات السيبرانية و القانون الدولي ،دراسة منشورة بتاريخ (٢٠١٢/٥/٢)، ص١٣٤. على الموقع التالي:(أخر زيارة بتاريخ ٢٠١٦/٨/٣)

www.SID.ir/pdf

(90) Oona Hathaway, op. cit., p. 851.

(91) Rex Hughes, op. cit., p. 538.

(92) Greenberg, L. T., Information warfare and International Law, Mishawaka: National Defense University Press, 1998, p. 32.

(93)Oona Hathaway , op.cit ,p.851.

(٩٤) اللجنة الدولية للصليب الأحمر، "الملحقان "البروتوكولان الإضافيان لإتفاقية جينيف المعقودة في ١٢ آب أغسطس ١٩٤٩"، مصدر سابق، المادة (٤٨)، ص٤٠.

(٩٥) حماية الأعيان المدنية في القانون الدولي الإنساني، ٢٠٠٨ بحث منشور على الموقع: (آخر زيارة بتاريخ ٢٠١٦/٩/١)

http://www.mezan.org/uploads/files/8798.pdf

(96) Vida M. Antolin-Jenkins, Defining the parameters of cyberwar operations: Looking for law in all the wrong places? 51 Naval, REV, 132, 140, (2005).

(٩٧) اللجنة الدولية للصليب الأحمر، تقرير عن القانون الدولي الإنساني والنزاعات المسلحة المعاصرة، المؤتمر الدولي الثاني والثلاثون للصليب الأحمر والهلال الأحمر (قوة الانسانية)، جنيف، سويسرا ٨-١٠ كانون الأول/ديسمبر ٢٠١٥. رقم الوثيقة 32IC/15XXX.

(٩٨) أحمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٢.

(99) Oona Hathaway, op. cit., p. 854.

(100) Antonio Gessese, "The Martens Clouse: Half a loaf or simply pien the sky? " EJIL (2000), Vol. III, No. 1, p. 187-194.

(١٠١) اللجنة الدولية للصليب الأحمر، "الملحقان، البروتوكولان الإضافيان إلى إتفاقيات جينيف الأربعة لعام ١٩٤٩، مصدر سابق، ص١١٨.

(102) ICJ Nuclear weapons Advisory opinion, op. cit., Dissenting opinion of Judge Shahabuddeen ,pp. 22-23.

(103)ICJ Nuclear weapons Advisory opinion , para 78.

(104) Ibid , para 86.

(١٠٥) احمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٤.

المصادر

المصادر العربية
أولا: الكتب
١. توليو ستيف وشمالبرغر توماس، "قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبناء الثقة"، معهد الأمم المتحدة لبحوث نزع السلاح، منشورات الأمم المتحدة، ٢٠٠٣.
٢. عمر بن يونس، المجتمع المعلوماتي، الدار العربية للموسوعات، بيروت، ٢٠١٠.
٣. محمد طلعت الغنيمي، الوسيط في قانون السلام، منشأة المعارف، الاسكندرية، ١٩٩٣.
ثانيا: الرسائل و الأطاريح
١. سراب ثامر احمد، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة من متطلبات نيل درجة الدكتوراه في القانون العام، جامعة النهرين، كلية الحقوق، ٢٠١٥.
٢. غازي عبد الرحمن هيان الرشيد،الحماية القانونية من جرائم المعلوماتية (الحاسب و الإنترنت)،إطروحة لنيل درجة الدكتوراه في القانون ،الجامعة الإسلامية في لبنان،كلية الحقوق، ٢٠٠٤.
ثالثا:البحوث و الدراسات
١. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،مجلة المحقق الحلي للعلوم القانونية و السياسية، جامعة بابل، السنة الثامنة، العدد الرابع، ٢٠١٦.
٢. إرشادات الإسكوا للتشريعات السيبرانية ،مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية ،بيروت ،٢٠١٢.
٣. بدر محمد هلال ابو هويل، جريمة العدوان في القانون الدولي، دراسة لإستكمال متطلبات النجاح في مساق القانون الدولي، جامعة آل البيت، كلية الدراسات العليا، الأردن، ٢٠١٢.
٤. روبرت كناكي، حوكمة الإنترنت في عصر إنعدام الأمن الإلكتروني، سلسلة دراسات عالمية، مركز الإمارات للدراسات والبحوث الإستراتيجية، أبو ظبي، العدد ٩٥، ٢٠١١.
٥. فرانسوا بونيون، الحرب العادلة وحرب العدوان والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر، مختارات من اعداد عام ٢٠٠٢.
٦. اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني (إجابات عن أسئلتك)، ديسمبر ٢٠١٤
٧. مايكل ن.شميث ، الحرب بواسطة شبكات الإتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) و القانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من أعداد ٢٠٠٢.
٨. مصطفى عصام نعوس، سيادة الدولة في الفضاء الإلكتروني ، مجلة الشريعة و القانون ، جامعة الإمارات العربية المتحدة ، كلية القانون ، السنة السادسة و العشرون ، العدد ٥١ ، يوليو ٢٠١٢.
٩. نبيل علي وفادية حجازي، الفجوة الرقمية رؤية عربية لمجتمع المعرفة، سلسلة عالم المعرفة، العدد ٣١٨، (الكويت، المجلس الوطني للثقافة والفنون والآداب، ٢٠٠٥).
رابعا: الصكوك و الوثائق الدولية
١. البروتوكول الإضافي لإتفاقية الجريمة المعلوماتية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهة الأجانب المرتكبة عبر أنظمة الكمبيوتر، ٢+٨ يناير ٢٠٠٣، على الموقع
http://Conventions.Coe.int/treaty/fr/Treaties/Html/189.htm
٢. التوصية الصادرة عن مجلس أوروبا رقم R(95)13 بتاريخ ١١/سبتمبر ١٩٩٥.
٣. اللجنة الدولية للصليب الأحمر، "القانون الدولي المتعلق بسير العمليات العسكرية، مجموعة اتفاقيات لاهاي وبعض المعاهدات الأخرى" ، جنيف، ط ثانية، سبتمبر/ايلول ٢٠٠١.
٤. اللجنة الدولية للصليب الأحمر، "الملحقان" "البروتوكولان الاضافيان إلى اتفاقية جينيف المعقودة في ١٢ آب اغسطس ١٩٤٩"، جنيف، سويسرا، ط٤، ١٩٩٧.

٥. اللجنة الدولية للصليب الأحمر، تقرير عن القانون الدولي الإنساني والنزاعات المسلحة المعاصرة، المؤتمر الدولي الثاني والثلاثون للصليب الأحمر والهلال الأحمر (قوة الانسانية)، جنيف، سويسرا ٨-١٠ كانون الأول/ديسمبر ٢٠١٥. رقم الوثيقة 32IC/15XXX.

٦. مجلس أوروبا، إتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، مجموعة المعاهدات الاوربية رقم ١٨٥،بودابست، عام ٢٠٠١.

٧. ميثاق الأمم المتحدة على الموقع الرسمي www.un.org>charter-united-nations

خامسا: المواقع الإلكترونية

١.حماية الأعيان المدنية في القانون الدولي الإنساني، ٢٠٠٨ بحث منشور على الموقع: (آخر زيارة بتاريخ ٢٠١٦/٩/١)
http://www.mezan.org/uploads/files/8798.pdf

٢. اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، تقرير تشرين الاول/اكتوبر ٢٠١١، متاح على الموقع الرسمي: www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st international-conference/31-int.conference-ihl-challenges-report-11-5-1-2-en.Pdf.

٣. مقال منشور بعنوان الحروب الالكترونية بتاريخ ٢٨/مايو/٢٠١٢ على الموقع الالكتروني:(آخر زيارة بتاريخ ٢٠١٦/٨/١٢)
http://whitehatssecurity.com/28/05/2012/cyberwars

٤. عادل عبد الصادق، الفضاء الالكتروني واسلحة الانتشار بين الردع وسباق التسلح، ١٥/مايو/٢٠١٥، مؤتمر حروب الفضاء السيبراني، متوفر على الموقع الالكتروني-الفضاء: (أخر زيارة بتاريخ ٢٠١٦/٧/٢٧)
Http://Seconf.wordpress.com/2015/05/15

٥ .ابتسام محمد العامري،منظمة شنغهاي للتعاون الإقليمي،١٤/ آذار/٢٠١٣ متاح على الموقع
http://Icis.Uobaghdad.edu.iqLuploads/workshop

المصادر الأجنبية

١.الإنجليزية

First:the Book

1. Martin C. Libicki ,Cyber deterrence and Cyber war ,Project Air Force, prepared for United States Air Force , 2009.

2. Micheal S. Fuertes, "Cyber warfare, Unjust Actins in a just war" Florida International University, Full 2013.

3. Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schojlberg, "Global Cyber Deterrence views from China, the U.S., Russia, India, and Norway", The East West Institute, printed in the United States, 2010.

second:researches & studies

1. Michael N. Schmitt, Computer network attack and the use of force in International Law: Thoughts on normative framework, International Review of the Red Cross,No.846, 30/6/2002.

2. A. Randelzhofer, "Article 2(4)", in: Simma, B. (ed), The Charter of the United Nations: A commentary. Vol. 1, 2002.

3. Antonio Gessese, "The Martens Clouse: Half a loaf or simply pien the sky?' EJIL (2000), Vol. III, No. 1.

4. Daniel. B. Silver, Computer Network Attack as a Use of Force Under article 2(4) of United Nations Charter, in computer network attack and international law 73, 2002.

5. Gray Sharp, in Stephanie G. Handler, The new cyber Face of the Battle, Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, vol. 48, 2012.

6. Greenberg, L. T., Information warfare and International Law, Mishawaka: National Defense University Press, 1998.

7. Ingrid Detlar, The Law of War, Cambridge , Cambridge University press ,2003.

8. K. Saalbach, "Cyber war, Methods and Practice", version 2.0, university of Osnabruck-17 Jun 2014.

9. Marco Roscini , "Threats of Armed Force on contemporary International Law". Netherlands International Law Review, No. 54, 2007.

10. Martin C. Libicki ,Cyber deterrence and Cyber war ,Project Air Force, prepared for United States Air Force , 2009.

11. Matthew J. Sklerov, solving the Dilemma of state Responses to cyber Attacks: A Justification for the use of Active Defenses against states who Neglect their Duty to prevent, 201 MIL. L. REV., fall 2009, at 1.

12. Murice Aubert,"The ICRC and the problem of excessively or indiscriminate weapons" Extract print from ICRC, No. 279, Nov-Dec. 1990.

13. Nils Melzer, "Cyber warfare and International Law", 1 DEAS for Peace and Security. UNIDIR Researches, 2011.

14. Oona A. Hathaway, Rebecca Crootof , Philip Levitz, Haley Nix, Aileen Nowlan , William Perdue & Julia Spiegel, "The law of Cyber-Attack", California law review, 2012.

15. Rex Hughes , "A Treaty for cyber space", International Affairs Journal, vol. 86, No. 2, 2010.

16. Sean P. Kanuck, Recent Development: Information warfare: New Challenges for public International Law, 37 Harvard International Law Journal, l. 272, 290 ,1996.

17. Vida M. Antolin-Jenkins, Defining the parameters of cyberwar operations: Looking for law in all the wrong places? 51 Naval, REV, 132, 140, (2005).

18. Wolff Heintscble Von Heinegg, Territorial Sovereignty and Neutrality in cyberspace, U. S. Naval war college, 2013 volume 89.

Third: documents

1. Micheal N.Schmitt. William H.Boothby. Wolff Heintschel Von Heinegg. Thomas C.Wingfield. Eric Talbot Jensen. Seen Whatts. Louise Arimatsu. Genevieve Bernatchez. Penny Cumming. Robin Geiss. Terry D.Gill. Derek Jinks. Jann Kleffner. Nils Melzer & Kenneth Whatkin , "Tallinn Manual on the International Law Applicable to Cyber warfare", Cambridge University Press, First Publishes, 2013.

2. ICJ, Military and paramilitary activities in and against Nicaragua (Nicar .v. U.S.), 1986, ICJ. 14, (June 27).

3. ICJ Nuclear weapons Advisory opinion, legality of threats or use of Nuclear weapons. Advisory opinion, 1996, I.C.J. 226 (8 July).

4. UN, "Year book of the International Law commission" vol. II, part 1, 1980.

5. UN.General Assembly.Res. 3314, Dec,14,1974.

6. UN.General Assembly, Res. 3314, U.N. Doc. A/RES/3314, (Dec. 14, 1974).

7. UN.General Assembly Rec. 25/2625, U.N. Doc .A/RES/25/2625 (Oct. 24, 1970).

8. UN.General Assembly. Res.37/10, U.N. Doc .A/RES/37/10 (Nov., 15, 1982).

Forth:Web-stes

1.U. S. Dept's of Def., An assessment of Intgernational Legal Issues in information operation 18 (1999). Available at:

http://www/au/of.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf,reprinted in76 INT'S L. Stud. 459, 483 (2002).

2. Robert McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program?: pc word", Sep. 12. 2010, at this link:

www.Sscenter/article/205827/was-stuxnet-built-to-attack-iran's-nuclear-program.html.

3.Mark Clayton, "Stuxnet malware is weapon out to destroy Iran's Bushehr nuclear plant? The Christian Science Monitor, Sep. 21.2010, at this link: www.Csmonitor.com. U.S.A./2010/0921/Stuxnet-Malware-is....

4. Cyber Warfare(2015) available at http://www.rand.org/topics/cyberwarfare.html

٢.الفارسية

اولا: الدراسات والبحوث

١. احسان كيان خواه و سعيد علوي وفا، مفهوم الأمن السيبراني، مجموعة مقالات المؤتمر الوطني الأول للفاع السيبراني، طهران/ايران، ٢٠١٢.

٢. قاسم ترابي، تطور إستراتيجية حلف الشمال الأطلسي في مواجهة الحرب السيبرانية الأسباب و الأبعاد و المكونات، دورية مطالعات راهبردي، السنة ال١٨، العدد الأول، ربيع ٢٠١٥.

ثانيا: الرسائل و الأطاريح

١. محمد علي رعايت كننده فلاح، الحرب السيبرانية و تهديد الأمن القومي لجمهورية ايران الإسلامية، أطروحة دكتوراه، جامعة آزاد اسلامي، كلية الآداب و العلوم الإنسانية، قم/ايران، ٢٠١٢.

ثالثا: المواقع الإلكترونية

١. علي قاسمي و ويكتور بارين جهار بخش، الهجمات السيبرانية و القانون الدولي ،دراسة منشورة بتاريخ (٢٠١٢/٥/٢)، ص١٣٤. على الموقع التالي:(أخر زيارة بتاريخ ٢٠١٦/٨/٣)

www.SID.ir/pdf